SDREN Connection Approval Process

Purpose

This Secret Defense Research and Engineering Network (SDREN) Connection Approval Process (CAP) establishes the terms and conditions for connecting to the SDREN, a part of the High Performance Computing Modernization Program's (HPCMP) network. The organization and the SDREN's site Designated Approving Authority (DAA) must concur with all terms of this SDREN CAP as a prerequisite to receiving and retaining an SDREN connection. Access to the SDREN requires access to the DREN, either through a direct connection or as a tail connection using approved protected distribution system (PDS) or National Security Agency (NSA) Type 1 hardware encryption.

SDREN Communities of Interest

The organization/agency wishing to receive SDREN access must belong to one of the following HPMCP communities: Science and Technology, Test and Evaluation, Missile Defense Agency, Defense Threat Reduction Agency, or Modeling and Simulation. Furthermore, there must be a mission requirement for high capacity/bandwidth, low latency network connectivity in direct support of these communities. Contractor sites requesting SDREN connectivity must be sponsored by a government agency, and the access must be within the scope of their contract. All sites, government and contractor, must be accredited in accordance with DODD 8500.1 for processing and storing data up to Secret System High Level NOFORN and must follow all current DoD guidelines for Access Distribution Points (ADP) systems. Documentation in support of accreditation must be developed in accordance with the DITSCAP, DODI5200.40.

Secret DREN (SDREN)

The SDREN is a virtual private network overlay of the DREN using Fastlane KG-75 and Taclane KG-175 NSA Type 1 encryptors and a common HPCMP Secret System High key. A SDREN site is defined as a site that communicates directly with other SDREN sites via this HPCMP common key. Before a site is issued the common key, it must complete the SDREN CAP and receive an authority to connect to the SDREN from the HPCMP DAA. An SDREN site may be connected to tail sites via links protected with NSA Type 1 encryptors and a key other than the HPCMP common key. Before traffic from any of these tails can be forwarded onto the SDREN, however, the tail must also complete the SDREN CAP and receive an authority to transmit data from the HPCMP DAA. The same applies to tails of tails and so on.

Note that SDREN is not synonymous with classified communications across the DREN cloud. Any NSA approved Type 1 encryptors and appropriate keys can be used to protect classified data over the DREN. A Memorandum of Agreement (MOA) in accordance with DODD 8500.1 must govern such communications and a copy of the MOA must be on file with the HPCMP. If the sites are not using the HPCMP common key, they are not part of the SDREN and it is not necessary to complete the SDREN CAP.

SDREN CAP

The following sections outline the steps in the SDREN CAP. Note that DREN connectivity is a prerequisite for SDREN connectivity, and the DREN has its own connection approval process. Use of the SDREN will not be authorized and a HPCMP common key will not be issued until the site has completed the connection approval process for both the DREN and the SDREN. To learn more about the DREN CAP or to check the status of DREN connectivity, contact the DREN team at (703)812-8205 or networking@hpcmo.hpc.mil.

1.0 SDREN Requirement

The organization/site must have validated classified networking requirements for HPCMP centrally funded access to SDREN. Buy-in sites must provide a written justification for SDREN use. This justification should include a list of sites to which connectivity is required and any bandwidth or latency requirements that support approval of SDREN connectivity. Both the sustained and burst bandwidths should be included. The justification should also include contact information for the site's DAA, ISSM, networking lead, and COMSEC custodian. For contractor sites, the justification must come from the contracting officer and must include the contract number, expiration date, and contact information for the contracting officer and contracting officer's representative.

2.0 HPCMP Funding Validation

For HPCMP funded sites, the classified networking requirement will be checked against the HPCMP requirements database. Buy-in sites will need to identify their funding source, and provide a Military Interdepartmental Purchase Request (MIPR) to the DREN Program Manager to cover costs for bandwidth usage at their site and all other sites they need access to as well as to cover costs for SDREN Network Operations Center (NOC) support and security assessments at their site.

3.0 SDREN MOA Sent

Once it is determined that the requirement for SDREN connectivity is valid, the information gathered from the site will be forwarded to the SDREN NOC. The NOC will verify contact information with the site and provide a copy of the SDREN MOA with the appropriate signature blocks and the SDREN consent to monitor statement. If the site is HPCMP centrally funded, a Fastlane or Taclane encryptor and DTD will also be sent by the NOC. In order to receive a Fastlane or Taclane, the site must have a valid COMSEC account. The COMSEC custodian, COMSEC account number and street address will be verifie d before any COMSEC devices are shipped. Please contact the SDREN NOC COMSEC custodian for a COMSEC account validation form. Return the form to the SDREN NOC when completed.

4.0 Required Documentation

Once the proper persons have signed the SDREN MOA and consent to monitor, they should be returned along with the security documentation described below to the SDREN NOC. Address the package to:

WareOnEarth Communications Inc.
SDREN NOC
2457 Aviation Ave. Suite 200
North Charleston SC 29406

The following documents should be included in the package:

4.1 Letter of Accreditation

Letters of accreditation signed by the site DAA must be provided for all AISs or LANs connecting to the SDREN. Each letter should specify accreditation at the Secret level System High mode. An interim authority to operate is acceptable, but must still be signed by the site DAA and specify why full accreditation has not yet been granted. For contractor sites, the accreditation will not be considered valid past the contract expiration date.

4.2 Network Diagram showing all tails

A network diagram showing the full path to the DREN Service Delivery Point (SDP) must be provided showing all classified enclaves and all external access as well as any tails, whether the tails are to access SDREN or not. Only registered ".smil" network address space shall be used on AISs connected to the SDREN. Sponsoring government agencies should provide appropriate IP addresses and NSAP space to contractor sites. If addresses are not available they can be requested from the HPCMP.

4.3 MOAs for any tails

Communications with any tails identified on the network diagrams must be governed by an MOA signed by both local DAAs. A copy of the MOA for each tail must be provided to the SDREN NOC, whether the tail will be accessing the SDREN or not.

4.4 PDS Approval letter

A letter of approval must be presented for any PDS included in the local classified infrastructure.

5.0 Accreditation Package Validated

The SDREN NOC and HPCMP will examine the accreditation packages for completeness and accuracy. Any portions missing will result in a delay in access to the SDREN. The site will be contacted if additional information is required..

6.0 IATC or IATTD

Once the accreditation info is complete, the HPCMP DAA will sign the MOA and grant an Interim Authority to Connect (IATC) to the SDREN in the case of an SDREN site, or an Interim Authority to Transmit Data (IATTD) in the case of a tail. A copy of each will be sent to the site's DAA The IATC is valid until an HPCMP security assessment is performed, or for a maximum of one year.

7.0 SDREN Key Issued

The SDREN NOC will be sent a copy of the site's MOA and IATC or IATTD. For an IATC, the NOC will furnish the HPCMP common key to the site's COMSEC custodian. The NOC will notify every other SDREN site that the new site has come on-line.

8.0 Security Assessment Scheduled

The site will be scheduled for an HPCMP security assessment to be performed before the IATC expires.

9.0 Notifications of Changes

The site will immediately notify the HPCMO of any changes in their secret enclave. New or inactive tails, new classified systems, major changes in network configuration and any other changes affecting accreditation status must be reported.

10. Security Assessment Performed

An HPCMP security assessment will be performed at the site to certify the accreditation on which their interim authority is based. The following seven disciplines will be examined: Physical Security, Personnel Security, Administrative Security, TEMPEST, Communications Security, Information Security, and Information Systems Security. Test procedures will include inspection of the facility, interviews with site personnel, system scans, and ad hoc testing on select systems at the discretion of the test director. THERE WILL BE NO SNIFFING OF CLASSIFIED TRAFFIC DURING THESE ASSESSMENTS.

11.0 Addressing Assessment Findings

The site must address any findings resulting from the security assessment. A formal response to the HPCMP DAA is required. The HPCMP DAA will determine if the findings have been adequately addressed.

12.0 ATC or ATTD Granted

The HPCMP DAA grants a full Authority to Connect to the SDREN, or an Authority to Transmit Data for tail sites, for up to three years. The site must continue to notify the HPCMP of any significant changes in their configuration. Additional security assessments are required whenever there is a change affecting the site's accreditation, but at least every three years.

Fastlane/Taclane Key Management

All SDREN key management is done through the SDREN RED NOC.

SDREN NOC

The SDREN NOC provides a variety of services to SDREN sites such as key management, DNS, WAN real time statistics, routing/ARP diagnostics and a help desk.

SDREN NOC POCs are as follows:

Manager/Fastlane/Taclane/Network Support: Mark Heck (843)529-0678 ext 107
COMSEC Custodian/Fastlane/Taclane/Key Management: Tony Wespy (843)529-0678 ext. 104
Fastlane/Taclane/Key Management: Melony Bell (843)529-0678 ext.118

Updated November 8, 2002